Remarks

Status of Claims:

Claims 1-39 remain for examination.

Rejections under 35 U.S.C. §112:

Claims 36-39 stand rejected under 35 U.S.C. § 112. By way of the instant amendment, claims 36-39 have been amended to remove the grounds of rejection as stated in paragraphs 4-7 of the outstanding office action. It is submitted that all of applicant's claims clearly comply with the provisions of 35 U.S.C. ¶112.

Prior Art Rejection:

Claims 1-35 and 37 stand rejected under 35 U.S.C. § 103 as unpatentable over Duursma in view of Stevens. Further, claim 36 stands rejected under 35 U.S.C. § 103 as unpatentable over Stevens. Finally, claims 38 and 39 rejected under 35 U.S.C. § 103 as unpatentable over Duursma.

The examiner's rejections are respectfully traversed.

Duursma is a paper about (calculation of the order of Jacobian, an efficient addition algorithm}, etc. in $y^2 = x^p - x + d \cdots (1)$ (p is the characteristic of a definition object) as an example of specific hyper elliptic curve pointed out by line 19 of the page 2 of this application.

On the other hand, this invention relates to the calculation method of the order of Jacobian of a more complicated algebraic curve ($\alpha y^a + \beta y^b + k = 0 \cdots (2)$). Therefore, this invention introduces various distinctive methods which are not disclosed in the Duursma reference.

In addition, Stevens is related with the relation of the modular curve and elliptic curve which are not related to this invention at all.

In last paragraph of page 2, paragraph 1 and 2 of page 3 of Duursma, the general definition of hyper elliptic curve, the definition of the devisor and Jacobian, and the character of addition on Jacobian in hyper elliptic curve are described.

On the other hand, the description of "a Jacobian addition candidate value comuting..." of this invention pointed out in the Office action indicates the procedure which calculates the candidate value of Jacobian addition (Jacobi sum) $j^p(l,m)$ (line 6, page 42 of the specification) necessary in order to calculate the order of the Jacobian. "Jacobian addition" in this invention means the so-called "Jacobi sum, and is not the semantics of the addition in Jacobian.

The above-mentioned component of this invention is not described at all in Duursma.

In paragraphs 4, 5 of page 3, and paragraph 1 of pages 4 and 5 of Duursma, a definition and character of the general zeta-function are described.

On the other hand, the description of "an order candidate value comuting procedure computing...." pointed out in this invention pointed out in the Office action indicates the procedure which calculates the set of the candidate value of the order of the Jacobian using the above-mentioned Jacobian addition as a process for comprising secure cryptography from the curve defined by the above-mentioned formula (2).

Therefore, the above-mentioned feature of the applicant's invention are not described at all in the indication parts of Duursma.

In the section 3.5 of pages 7 - 8 of Duursma, the example computation of the order of Jacobian of hyper elliptic curve of the above-mentioned formula (1) is described.

The description of a security judging ... "and "a parameter deciding procedure ... "indicates the procedure for obtaining a secure algebraic curve to the algebraic curve of the more complicated above-mentioned formula (2). Duursma also does not disclose these features of applicant's invention.

Although it is indicated that the calculation method of Stickelberger element is disclosed in Stevens, the essence of this invention is not in the calculation method of Stickelberger element, but being in using Stickelberger element for calculation of the Jacobian addition j^p (refer to page 43 of the specification).

In order to better differentiate applicant's invention from the cited references, applicant has amended all of the independent claims to make it clear that the invention is directed to a secure parameter generating device in an algebraic curve cryptography having the definition expression of $\alpha Y^a + \beta X^b + 1 = 0$, which is formula (2) discussed above. With this claim modification, it is submitted that all of applicant's claims are clear distinguish applicant's invention over the prior art and that applicant's claims are patentable thereover.

Conclusions:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date 8-16-04

By

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257